Enhanced Bit Compressed Authentication Approach to Prevent False Data Injection Attacks and Energy Wastage in Route Nodes Over Wireless Sensor Network

Vinita Prashar
P.G Student in CSE Department,
Gurukul Vidyapeeth , Banur, Rajpura, Punjab, India

Abstract— **Sensor Nodes Offer a powerful Combination of Distributed Sensing, Computation and Communication. A sensor network is a static ad hoc network consisting of hundreds of sensor nodes deployed over an area to perform local computations based on information gathered from the surroundings. They lend them self to countless application but also offers a numerous challenges Each sensor node is equipped with a sensing device, a low computational capacity processor, and a limited battery-supplied energy. The main design issues for a sensor network is conservation of the energy available at each sensor node and Injecting false data attack is a well known serious threat to wireless sensor network. This Paper Of wireless sensor network introduce a E-BCA(Enhanced bit compression technique) scheme is used to save energy by early detecting data and injecting false data by using key authentication technique and time based technique that possibly minimize computation done by sink which reduce burden on sink and hence reduce energy consumption.**

Keywords-Wireless Sensor Network, False Data Injection, Gang Data injection, Management of Energy Waste, Bit Compression.

I. INTRODUCTION

Wireless sensor networks (WSNs) are ideal for environmental monitoring applications because of their low implementation cost, agility, and robustness to sensor failures. Sensor networks are primarily designed for real-time collection and analysis of low level data in hostile environments. For this reason they are well suited to a substantial amount of monitoring and surveillance applications. a large number of small sensing self-powered nodes which gather information or detect special events and communicate in a wireless fashion, with the end goal of handing their processed data at a base station. Sensing, processing and communication are three key elements whose combination in one tiny device gives rise to a vast number of applications .Sensor networks provide endless Opportunities, but at the same time impose formidable challenges. In sensor networks, adversaries can inject false data reports containing bogus sensor readings or nonexistent events from some compromised nodes. Such attacks may not only cause false alarms, but also drain out the limited energy of sensor nodes.

To overcome the problem of energy waste and false data injection we, propose a nobel enhanced bit compressed authentication (E-BCA) Scheme to overcome the problem of false data and energy waste in wireless sensor network. The E-BCA scheme achieves not only high filtering probability but also high reliability. The main highlight of this paper are, firstly we initialized the sensor nodes and then take a routing establishment by taking of K-neighbour nodes and then filtering false injection attack by key authentication and filtering gang injection attack by on the bases of time-out bases with the proposed mechanism, false data can be early detected and filtered by the en-route sensor nodes. We develop custom Java Simulator and use IED NETBEANS6.0 to demonstrate the effectiveness of the proposed E-BCA scheme in terms of en-routing filtering probability.

II. SUBJECT STRATEGY

This section first presents the architecture of a WSN. Next, the coordinator selection methods are presented. The routing model used in this study is then presented.

A. Architecture

A wireless sensor network consists of n sensor nodes in which nodes are divided into several clusters.

Let N={N0.N1,N2.....} are Taken as sensor nodes .Each Sensor node detects all neighbour nodes including the neighbour sensor nodes and forwarding nodes. Once it detects all neighbour nodes, depending upon the mobility of the sensor node, cluster head will be chosen. The sensor node, which has high mobility, acts as a cluster head. . The sink is one of the most powerful data collection devices, which has sufficient computation and storage capabilities and is responsible for initializing the sensor nodes and collecting the data sensed by these nodes.

But in over scheme, we assume Sensor node transmits sensed data to cluster head, cluster head then forwards to

forwarding node. Forwarding nodes checks for authentication of the received report. Forwarding node verifies the key value of sensor node and timestamp it forwards the data. If the timestamp or the authenticity breaches then the data will be discarded by forwarding node otherwise it will be delivered to base station.

Establish a key pool containing various random generated key value initialize each sensor node with a key value from the key pool. CNR Based MAC Generation S Sensor nodes receives key pair while establishing the connection, the key is taken randomly from the key pool Sensor node uses non-interactive key-pair establishment. Sensor nodes establish keys randomly from key pool. Sensor node establishes path to sink R_{N0}: $\{R_1 - R_2 \ldots R_l - \text{Sink}\}$ and the key is $\{k_{i1}, k_{i2} \ldots k_{il}, k_{is}\}$

If then sensor node which receives the data believes that the data is true then the neighbour nodes also has the same ability to detect a true event as the source node and correctly judges the report m.

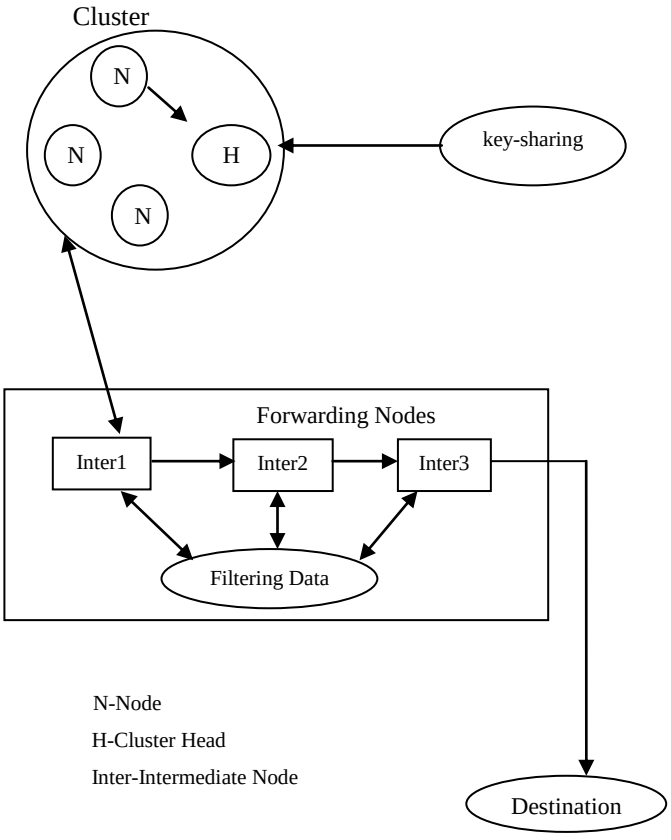


Figure 1. System Architecture

III. LITERATURE REVIEW

A. *Statistical En-route Filtering*

Ye et al. propose a statistical en-routing filtering mechanism called SEF. SEF requires that each sensing report be validated by multiple keyed message authenticated (MACs), each generated by a node that detects the same event. As the report being forwarded, each node along the way verifies the correctness of the MACs at earliest point. If the injected false data escapes the en-routing filtering and is delivered to the sink, the sink will further verify the correctness of each MAC carried in each report and reject false ones. To save the bandwidth, SEF adopts the bloom filter to reduce the MAC size. [9]

Issues in existing system

The filtering probability at each en-routing node is relatively low. Besides, SEF does not consider the possibility of en-routing nodes' compromise, which is also crucial to the false data filtering.

B. *Hop-by-hop authentication (IHA)*

Zhu et al. present an interleaved hop-by-hop authentication (IHA) scheme for filtering of injected false data. In IHA, each node is associated with two other nodes along the path, one is the lower association node, and the other is the upper association node. An en-routing node will forward receive report if it is successfully verified by its lower association node. To reduce the size of the report, the scheme compresses individual MACs.

Issues in existing system

The security of the scheme is mainly contingent upon the creation of associations in the association discovery phase. Once the creation fails, the security cannot be guaranteed. The symmetric keys from a key pool, which allows the compromised nodes to abuse these keys to generate false reports.

C. *Location-Based Resilient Secrecy (LBRS)*

Yang et al. proposed Location-Based Resilient Secrecy (LBRS), which adopts location key binding mechanism to reduce the damage caused by node compromise, and further mitigate the false data generation in wireless sensor networks.

Issues in existing system

To achieve en-routing filtering, additional 20 bytes authentication overheads are required.

D. *Location-aware end-to-end data security design (LEDS)*

Ren et al. propose more efficient location-aware end-to-end data security design (LEDS) to provide end-to-end security guarantee including efficient en-routing false data filtering capability and high-level assurance on data availability.

Issues in existing system

To achieve en-routing filtering, additional 20 bytes authentication overheads are required. It assumes that all the nodes can determine their locations and generate location-based keys in a short secure time slot.

E. *Public key based solution*

Zhang et al. provide a public key based solution to the same problem. Especially, they propose the notion of location-based keys by binding private keys of individual nodes to both their IDs and geographic locations and a suite of location-based compromise-tolerant security mechanisms.

F. *Bit-compressed authentication technology*

Bit-compressed authentication technology can achieve bandwidth-efficient. Canetti et al. use one-bit authentication to achieve multicast security. Source knows a set of keys each

recipient u knows a subset. When the source sends a message M, it authenticates M with each of the keys, using a MAC.

Issues in existing system

In Bit-compressed authentication, however, once the source is compromised, the scheme obviously does not work. Therefore, it cannot be applied to filter false data injected by compromised nodes in wireless sensor networks.

G. Becan Scheme

A novel bandwidth-efficient cooperative authentication (BECAN) scheme for filtering injected false data is deployed in existing system. Based on the random graph characteristics of sensor node deployment and estimate the probability of k-neighbours which provides the necessary condition for cooperative bit-compressed BECAN authentication technique. This scheme saves energy by early detecting and filtering the majority of injected false data with minor extra overheads at the en-route nodes. In addition, only a very small fraction of injected false data needs to be checked by the sink which largely reduces the burden of the sink.

Issues in existing system

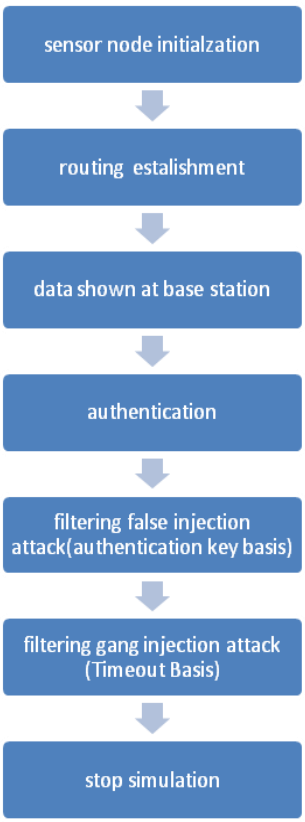
BECAN scheme is efficient for injecting false data by single attackers but not in case of group attackers. And has low reliability because if one report reaches the sink, the true event will successfully report else this scheme cannot filter injected false data. And if the path of length is too long authentication bit gets larger and hence reduce reliability as well as scalability

IV. MODULE DESCRIPTION

A. Sensor Node Initialization:

The sink deploys these initialized sensor nodes at a Certain Interest Region (CIR) in various ways, such as by air or by land. It is assumed that all sensor nodes are uniformly distributed in CIR after deployment. When these sensor nodes are not occupied by the reporting task, they cooperatively establish or adjust their routing to the sink either a shortest path or a path adapted to some resource constrains with some existing routing protocol. Note that, the established routing path can accelerate the reporting. Once an event occurs, a report can be immediately relayed along the established routing path.

Step: 1	Create a Base station in cluster 1
Step: 2	Create two forwarding nodes in Cluster1 and cluster 2
Step: 3	Create two sensor nodes in cluster 1
Step: 4	Base station, Forwarding node and sensor Nodes will have a unique identity Let sensor Nodes N={N0, N1, N2…}
Step: 5	Establish a key pool containing various Random generated key value
Step: 6	Initialize each sensor node with a key Value from the key pool.



Steps of Module Description

B. Routing establishment

In the proposed model, base station, forwarding node and sensor nodes has been designed. Base station receives message from sensor node. While establishing sensor node, the system identifies the cluster head, which is also one of the sensor node. Sensor node always sends data via cluster head, then to forwarding node and then to base station. For this sensor node and forwarding nodes must establish their neighbour nodes automatically.

C. Sensed results reporting

When a sensor node generates a report m after being triggered by a special event, e.g., a temperature change or in response to a query from the sink, it will send the report to the sink via an established routing. Assume that, the sensor (source) node N0 has sensed some data m and is ready to report m to the sink via the routing path R_{N0}: {R_1 - R_2 …R_l – Sink}. The source node N0 gains the current timestamp T, chooses k neighbouring nodes N_{N0} : {N_1,N_2, . . .,N_k} and sends the event m.

D. CNR Based MAC Generation

To filter the false data injected by compromised sensor nodes, the E-BCA scheme adopts cooperative neighbour router (CNR)-based filtering mechanism. In the CNR-based mechanism, when a source node N0 is ready to send a report m to the sink via an established routing path RN0: {R1 – R2 …Rl – Sink}, it first resorts to its k neighbouring nodes NN0 : {N1,N2, . . .,Nk} to cooperatively authenticate the report m, and then sends the report m and the authentication information MAC from N0 to the sink via routing RN0, where the sink initializes all sensor nodes, then each sensor node shares its

private key with the sink. When a compromised sensor node sends a false data to the sink, the false data can be filtered if there is at least one uncompromised neighboring node participating in the reporting.

Step: 1 Sensor nodes receives key pair while establishing the connection, the key is taken randomly from the key pool

Step: 2 Sensor node uses non-interactive key-pair establishment. Sensor nodes establish keys randomly from key pool.

Step: 3 Sensor node establishes path to sink RN0: {R1–R2…Rl – Sink} and the key is {ki1, ki2…kil, kis}

Step: 4 If then sensor node which receives the data believes that the data is true, then the neighbor nodes also has the same ability to detect a true event as the source node and correctly judges the report m.

E. Filtering false injection attack (Authentication Key Basis)

CNR Based MAC Verification

When each sensor node R_i, along the routing R_{N0} receives message m, timestamp T, and MAC key from its upstream node, it checks the integrity of the message m and the timestamp T. If the timestamp T is out of date, the received message m, timestamp T and MAC key will be discarded. Otherwise, R_i accepts the data will forward the message (m,T,MAC) to its downstream node, Otherwise, (m,T,MAC) will be discarded.

Step: 1 Sensor node uses bob-interative key pair establishment to compute shared keys with each node in $\{N_0, N_1, N_2, \ldots, N_k\}$ as $\{k_{01}, k_{02}\ldots k_{0l}, k_{0s}\}$

Step: 2 Sensor node receives message Timestamp and MAC key

Step: 3 Sensor node which receive the data check the time, the time is unmatched or old, then the data is discarded

Step: 4 Otherwise sensor node forwards the data to destination.

F. Filtering gang injection attack (Timeout Basis)

Sink Verification

When each sensor node R_i, along the routing R_{N0} receives message m, timestamp T, and MAC key from its upstream node, it checks the integrity of the message m and the MAC key established for each sensor node. The forwarding node checks the MAC key form key pool. If the verified key not matched, the received message m, timestamp T and MAC key will be discarded. Otherwise, R_i accepts the data will forward the message (m,T,MAC) to its downstream node, Otherwise, (m,T,MAC) will be discarded.

Step: 1 Sensor node uses bob-interative key pair establishment to compute shared keys with each node in $\{N_0, N_1, N_2, \ldots, N_k\}$ as $\{k_{01}, k_{02}\ldots k_{0l}, k_{0s}\}$

Step: 2 Base station receives forwarded message, Timestamp and MAC key from the upstream node

Step: 3 Base station which receive the data check node in cluster1 and region value is 100. Second forwarding node in cluster2 and region value is 70. Similarly two sensor node in cluster 1. Mobility value of sensor node is read by percentage value. The node, which is having high percentage, is considered to be the cluster head. Each sensor node acquires a key pair value form keys. Properties file and data for forwarding is taken from sensor. Properties file.

V. EXPERIMENTAL RESULTS

Filtering the false injected data is the main problem in wireless sensor network. The E-BCA scheme is used to filter the false data by verifying the unique MAC of every node.

We consider the implementation of a Base Station, two Forwarding Nodes and two Sensor Nodes. Base Station is created in Cluster1 and the Certain Interest Region (CIR) value is 1. First Forwarding node in cluster1 and region value is 100. Second forwarding node in cluster2 and region value is 70. Similarly, two sensor node in cluster1. Mobility value of sensor node is read by percentage value. The node, which is having high percentage, is considered to be the cluster head. Each sensor node acquires a key pair value form keys. properties file and data for forwarding is taken from sensor properties file.

We design a attackers in two forms, one is for giving wrong time value and another is for giving wrong key input. Sensor node first forwards the data to cluster head. Cluster head forwards to forwarding node. The filtering of false data is carried out in forwarding node. Once the forwarding node gets data from cluster head, it checks the received data, which contains a message, key pair, MAC key and timestamp.

There are two conditions are checked as attacker. One is when the forwarded data contain old timestamp it is considered to be false data attack. Another one is, when the forwarded sensor node's key is not matched with key pool value, and then it considered as the attacker. As the detection of attacker is identified in the earlier stages, that is, it is identified in the forwarding node itself and not in the base station, thus our application considered to be bandwidth efficient.

VI. CONCLUSION

In this paper, we have proposed a novel E-BCA scheme for filtering the injected false data. By theoretical analysis and simulation evaluation, the E-BCA scheme has been demonstrated to achieve not only high filtering probability But also high Reliability and multi reports on time out basis and key management basis and it easily find out the gang injection false data attack.Due to the simplicity and effectiveness, the E-BCA scheme could be applied to other fast and distributed authentication scenarios, e.g., the efficient authentication in wireless mesh network.

VII. FUTURE ENHANCEMENTS

In Future work it may be investigate how to prevent/mitigate the gang injecting false data attack from mobile compromised sensor nodes. Consider the scenario, when the wireless sensor node moves from one location to another location, it is difficult to identify the false data injection through this proposed mechanism. Thus to arrive an another

efficient model, based upon the location of sensor node and the keying material, the false data injection attack or gang injecting false data can be identified.

REFERENCES

[1] R. Szewczky, A. Mainwaring, J. Anderson, and D. Culler, "An Analysis of a Large Scale Habit Monitoring Application," Proc. Second ACM Int'l Conf. Embedded Networked Sensor Systems (Sensys '04), 2004.

[2] L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. Ninth ACM Conf. Computer and Comm. Security (CCS '02), 2002.

[3] R. Lu, X. Lin, C. Zhang, H. Zhu, P. Ho, and X. Shen, "AICN: An Efficient Algorithm to Identify Compromised Nodes in Wireless Sensor Network," Proc. IEEE Int'l Conf. Comm. (ICC '08), May 2008.

[4] X. Lin, R. Lu, and X. Shen, "MDPA: Multidimensional Privacy-Preserving Aggregation Scheme for Wireless Sensor Networks," Wireless Comm. and Mobile Computing, vol. 10, pp. 843-856, 2010.

[5] X. Lin, "CAT: Building Couples to Early Detect Node Compromise Attack in Wireless Sensor Networks," Proc. IEEE GLOBECOM '09, Nov.-Dec. 2009.

[6] K. Ren, W. Lou, and Y. Zhang, "Multi-User Broadcast Authentication in Wireless Sensor Networks," Proc. IEEE Sensor Ad Hoc Comm. Networks (SECON '07), June 2007.

[7] L. Zhou and C. Ravishankar, "A Fault Localized Scheme for False Report Filtering in Sensor Networks," Proc. Int'l Conf. Pervasive Services, (ICPS '05), pp. 59-68, July 2005.

[8] Z. Zhu, Q. Tan, and P. Zhu, "An Effective Secure Routing for False Data Injection Attack in Wireless Sensor Network," Proc. 10th Asia-Pacific Network Operations and Management Symp.
(APNOMS '07), pp. 457-465, 2007.

[9] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-Route Detection and Filtering of Injected False Data in Sensor Networks," Proc. IEEE INFOCOM '04, Mar. 2004.

[10] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-by- Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks," Proc. IEEE Symp. Security and Privacy, 2004.